HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 112 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, June 7, 2018

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Thursday, June 7, 2018

● (0850)

[*English*]

The Chair (Mr. Bob Zimmer (Prince Geo[illegible]ace River—Northern Rockies, CPC)): I call to order meeting 112 of the Standing Committee on Access to Information, Privacy and Ethics, pursuant to Standing Order 108(3)(h)(vii), study of breach of personal information involving Cambridge Analytica and Facebook.

Mr. Vickery, welcome back. Thanks for appearing at our committee again today.

Mr. Chris Vickery (Director of Cyber Risk Research, UpGuard, As an Individual): It's a pleasure to participate here.

The Chair: We'll start our first round with Mr. Erskine-Smith for seven minutes.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thanks, Mr. Vickery.

I really have one fundamental question. Have you reviewed the hard drive that you mentioned to us at your last attendance?

Mr. Chris Vickery: There's so much there that I'm sure there are still a few nooks and crannies that I have not peered at, but yes, I have reviewed a very large amount of it.

Mr. Nathaniel Erskine-Smith: You certainly have expertise that this committee does not have in reviewing that material. To the extent that you haven't reviewed the whole thing, you've reviewed a large portion of it, and upon that review, can you provide us the highlights of what you discovered in that review that you think is relevant for this committee, particularly in light of the fact that we are to have AIQ before us next week?

Mr. Chris Vickery: Yes. The fundamental overriding theme that hits me as I think back upon the overall bird's eye view of it is that there appear to be considerable efforts expended to make things not easily reviewable as far as Internet history goes and transaction history and data: where it goes, where it gets compiled, aggregated, and attributing the sources to everything. There seems to be a common theme of bringing lots of little things together and then letting them fall apart in a way that is not easily auditable. That could be done for security purposes. That could be done for obfuscation purposes. It makes me very suspicious, however.

For example, there is an underlying theme in the Ephemeral project—the name "ephemeral" sort of gives you an idea—and it utilizes channels and web sockets in ways that can communicate very covertly. That's not to say that it's necessarily something that is malicious on its face, but it is done in such a way that it's considerably difficult to prove beyond any doubt that a certain transaction has taken place in regular forensic means.

Mr. Nathaniel Erskine-Smith: I see some of your tweets indicating that AIQ had a Facebook app, that AIQ was spoofing U.S. phone numbers and contacting American voters. Those are two examples that I saw from some of your public comments. Are there other examples that we ought to know about that you've drawn from the material?

Mr. Chris Vickery: Yes. I would ask them very specifically why a developer commented that they needed to remove data that may have been gathered in violation of U.K. privacy laws. That is clearly almost an admission of guilt there. If you've collected something in violation of U.K. privacy laws and then you're getting rid of it, why did you do it in the first place?

Mr. Nathaniel Erskine-Smith: Who was the commenter?

Mr. Chris Vickery: I believe it was an anonymous comment, as far as I can tell. I may be able to look back and see who was working on that project, who would have probably commented that, but that would take a bit of looking on my part.

Mr. Nathaniel Erskine-Smith: When you first attended, your first reaction had been that there was information compiled from a number of different sources, and you referenced the RNC trust. I think you referenced even the Koch brothers. Upon further review, do you have a total sense of where all the information was gleaned from?

Mr. Chris Vickery: I know a lot of sources. I can't say for sure this is comprehensive because, of course, the sources have sources themselves. i360 is the name of the Koch brothers-funded or -run company that supplies lots and lots of data. The RNC data trust is clearly a large foundation where they're getting information or data from. There are indicators as far as field names go that L2 Political provided information, and I believe on Cambridge Analytica's website—not AIQ's website—they admit on their blog that L2 was the source.

Axiom was a source, I believe, that came out yesterday in Alexander Nix's testimony. When I group the AIQ and the Cambridge Analytica data together, there's so much interplay between the two that it's just intuitive that the datasets are intertwined, not to mention that clearly SCL IDs are in the field names of many of the imports.

Mr. Nathaniel Erskine-Smith: That's what I want to get at next with my question. What prompted this investigation at our end and around the world is the improper collection and sharing of information among Facebook, Kogan, and SCL. We're talking now of at least 87 million users around the world and over 600,000 in Canada. In your view, based upon your review of the database, it's clear that this information was accessed by AIQ and was part of this master dataset.

Mr. Chris Vickery: There's the possibility, and let me explain why that's a possibility. In the Ripon project, there are a few residual error logs of sorts where something went wrong during an import, and it logged what was happening. This import error log, as far as I can tell, has some examples of what it was importing from servers called SCLCruiseRipon.com scoring, I believe.

In there it has OCEAN psychographic scores, and it was pulling from a domain that is registered to Alexander Nix. I don't know where they were getting these psychographic scores from. Not every single entry had them, but many of them did. In the scripts that are pulling it, the scripts have a little field that says "if available" next to the psychographic scoring. If many of them have the psychographic scoring and many of them do not, it raises the question of whether they were pulling from that 87 million, and whether those were the ones that had the psychographic scores.

● (0855)

Mr. Nathaniel Erskine-Smith: If SCL and Nix are involved, far from being a possibility, it would appear likely that this database is drawn from that information.

Mr. Chris Vickery: I would agree. It is likely. I don't have any special communications from them confirming it, but I'm highly suspicious.

Mr. Nathaniel Erskine-Smith: That's all I have.

The Chair: Next up for seven minutes is Mr. Gourde.

[*Translation*]

Mr. Jacques Gourde (Lévis—Lotbinière, CPC): Thank you, Mr. Chair.

Mr. Vickery, you talked about data collection. What kind of data about people's private lives can be found in this software?

[*English*]

Mr. Chris Vickery: What types of fields? Is that the question?

[*Translation*]

Mr. Jacques Gourde: Earlier, you said that privacy data had been deleted. What did the data consist of? Was it phone numbers, dates of birth, bank account numbers?

[*English*]

Mr. Chris Vickery: I would have to go back and review that script. It was titled "salt the earth", and I remember the comment that was made in there because it stands out in my head, somebody's comment that it may have been in violation of U.K. privacy laws, but the exact fields that were then being stripped out, I don't have in my head.

[*Translation*]

Mr. Jacques Gourde: What you have provided to us seems rather complicated to understand. Is it the coding or how it's organized that makes it harder to understand?

[*English*]

Mr. Chris Vickery: It partially may be difficult to understand because it's the exact hard drive, or a copy of it, that I gave to the U. K. committee. In the U.K. committee private session, I was able to explain things a little and give some context. That may be where some of the confusion is coming from as I haven't sat with you guys and given any context to it. It also may be a bit confusing because this is not an unnecessarily intuitive click-click-click, window-window-window type of software. You have to be somewhat familiar with Git and decompression software and web development to have an idea of the interplay between many of these files and the way it commits and builds work.

[*Translation*]

Mr. Jacques Gourde: Could this software be provided to the committee so that we can understand what was on the hard drive?

[*English*]

Mr. Chris Vickery: Yes, they are free, open-source software. I can give you a list of them. If you have a tech team at all set up, I'm sure they will be able to dive right in.

[*Translation*]

Mr. Jacques Gourde: Did this software end up in the hands of several companies or was it limited to only a few of them?

[*English*]

Mr. Chris Vickery: I think we're getting into a bit of a dual answer here. There is software that are frameworks, that are open source and available to everyone in the world, and then there are projects that are made from that open-source software that AIQ tailored.

Are you talking about the AIQ-tailored ones, built from the frameworks, or the ones that are open source and available to the world?

[*Translation*]

Mr. Jacques Gourde: Actually, I wasn't talking about the software, but rather the information that was on the hard drive and that you provided to us. Was that information in the hands of several companies or was it in the hands of one particular company that at least tried to keep the information confidential?

● (0900)

[*English*]

Mr. Chris Vickery: The hard drive that you have is pulled directly from the GitLab instance at gitlab.aggregateiq.com. That would have been data held by AggregateIQ. However, they did incorporate a lot of scripting and software that is available on the open Internet.

I think the answer to your question is that this is internal AggregateIQ data. The overall philosophical answer is that anybody in the world could have accessed it, both because it was open and exposed on AIQ's side, and because they built it using software, primarily frameworks, that are available to the public. It's a bifurcated answer.

[*Translation*]

Mr. Jacques Gourde: Was the level of security this company assigned to the personal data on the hard drive high, medium or low?

[*English*]

Mr. Chris Vickery: As far as what I gave to you guys, the amount of security that was present was nothing. There was no security whatsoever guarding it. I wouldn't assign any level of security. There are user names, passwords, and network locations present, which could have been seen by anybody in the entire world.

[*Translation*]

Mr. Jacques Gourde: Unbelievable. So all the information on these hard drives could have ended up in the hands of anyone who was interested in using it for other purposes, quite simply.

[*English*]

Mr. Chris Vickery: Exactly. Yes, that is the very disturbing truth.

[*Translation*]

Mr. Jacques Gourde: Thank you. I'm done.

[*English*]

The Chair: Thank you, Mr. Gourde.

We'll go next to Mr. Boulerice. You have seven minutes.

[*Translation*]

Mr. Alexandre Boulerice (Rosemont—La Petite-Patrie, NDP): Thank you very much, Mr. Chair.

Mr. Vickery, thank you very much for appearing before our committee again, only a few months after your last appearance.

Much has been said about Cambridge Analytica, AIQ and SCL. In your opinion, what is the extent of this underground world of data exchange that can be used for political purposes? Are we talking about these entities simply because we stumbled upon them or because there were a few whistleblowers? Are there only these entities or is this the tip of the iceberg of a phenomenon much larger and broader than we could imagine?

[*English*]

Mr. Chris Vickery: It is my belief that what you just said there is most likely the truth, that this is a beginning to something much larger. Even though it's a very big beginning, I believe there is a fairly good chance that before this is over, we will find ties to additional countries that have not really been recognized in the media, as well as various special interest groups in the United States —perhaps in Canada, but definitely within the United States—that have been taking advantage of this set of data, maybe not knowing exactly where it comes from. I believe there is a very large machine at work here, and we have not seen all sides of it.

[*Translation*]

Mr. Alexandre Boulerice: In your opinion, how could we, as a state and a government, search and find other organizations or companies that exchange or use data in this way, for political purposes, to interfere in election campaigns? Should we start a big manhunt?

[*English*]

Mr. Chris Vickery: I believe that perhaps the best way to go at this is much the same way that classically the United States has worked to rout out mob families. You put pressure on the people that you have strong evidence against, get them to turn on their co-conspirators and get the inside information, and keep flipping the dominoes down the chain until all the truth comes out. This is being done in such a way that it's hard, unless you have inside information or there's a huge mistake like what I discovered. It's hard to get inside information into investigators' hands.

● (0905)

[*Translation*]

Mr. Alexandre Boulerice: But depending on what you say, once a breach has been made, it can be used to dig and find all the ramifications.

[*English*]

Mr. Chris Vickery: I believe we have a beachhead, if that's what you're talking about, to begin a foothold, in another way to phrase it, to start really digging in. Yes, I believe we have established a foothold.

[*Translation*]

Mr. Alexandre Boulerice: Thank you.

My next question is from the perspective of the Canadian Parliament, or perhaps Elections Canada. We value the integrity of our electoral system. We wouldn't want to see foreign powers interfere in our election campaigns and use our citizens' personal data to influence electoral behaviour, people's perceptions or even election results.

However, I have the impression that states are very heavy and very slow institutions. Here, for example, until very recently, MPs had to send authorisations by fax. It's a bit like running on roller skates behind a Ferrari and being constantly late.

What advice would you give us to ensure that our legislation to protect our citizens is up to date and appropriate?

Here, the whole process is a bit archaic. It's not very modern, and it's generally quite slow.

[*English*]

Mr. Chris Vickery: One angle that I believe, specific to the Canadian side of things, you have an advantage on really is that AggregateIQ is under Canadian jurisdiction. If you can get to the bottom of the AggregateIQ involvement in this whole situation, you can have some very good inside insight into, "Okay, they did this. How could we have seen this coming? How could we have seen some red flags? What did they do, and how did they get to this level of involvement without our knowing?" and put in place some stopgaps to prevent that sort of thing from happening in the future.

I believe you actually are in a power position, as far as that goes.

[*Translation*]

Mr. Alexandre Boulerice: That's good to know. Thank you.

Do you think the solutions lie more with investigations or more with legal or legislative protections?

[*English*]

Mr. Chris Vickery: I believe regulation, such as [*Technical difficulty—Editor*] is going to be very useful in protecting the public from abuses happening. If Canada wants to look into the GDPR model and you subscribe to it and pass something of your own, I'm very much in favour of regulation that has teeth behind it, so that it can be enforced. When there is an egregious violation of whatever law gets put in place, make an example of the companies that are the egregious violators and make others afraid to do it.

[*Translation*]

Mr. Alexandre Boulerice: It's a bit like what you were saying earlier about how to take on mafia families.

Mr. Chair, how much time do I have left?

[*English*]

The Chair: You have about 30 seconds.

[*Translation*]

Mr. Alexandre Boulerice: You are in the United States and we are in Canada. How would you rate our level of security in terms of the integrity of our electoral system? Are things going well or are we obviously threatened?

[*English*]

Mr. Chris Vickery: I have a quick question. Is Canada considering either phone-in or Internet voting?

[*Translation*]

Mr. Alexandre Boulerice: No, not yet.

[*English*]

Mr. Chris Vickery: Okay. Stay away from that. Use paper ballots with audit trails. As long as you're using paper ballots with audit trails, you're relatively on the right track.

[*Translation*]

Mr. Alexandre Boulerice: Thank you very much, Mr. Vickery.

[*English*]

The Chair: Next up for seven minutes is Mr. Saini.

Mr. Raj Saini (Kitchener Centre, Lib.): Good morning, Mr. Vickery. I want to follow up on some questioning from my colleague, Mr. Erskine-Smith, just to be clear.

You have discovered evidence that AIQ has been spoofing caller ID numbers in calls to American voters. Can you please explain to us what the evidence is and why that's a problem for them?

● (0910)

Mr. Chris Vickery: In the commentary of the developers writing to each other, they state that they are setting the caller ID differently from the truth, because if they call somebody it gives them the ability to have the person calling back on that number be routed to a different line. That could either be a voice mail message or something else—just not the same number that actually called them.

That is a problem as far as the U.S. side of things is concerned, because it is my understanding that the ability to do that is highly restricted to law enforcement situations, at least here in the U.S. Here, anybody spoofing caller ID information could face a lot of penalties, at least if it's aimed towards Americans. I'm not an attorney or a prosecutor, but that's my understanding.

Mr. Raj Saini: I'm going to quote your recent tweet that Chris Wilson, who I believe is a volunteer at the Leadership Institute, "has a huge AggregateIQ involvement". Can you explain what you mean by that?

Mr. Chris Vickery: Chris Wilson is the head of WPA Intelligence, formerly known as WPA Opinion Research. The WP is Wilson Perkins, I believe, and he's the "W" in WPA. They worked very closely with AggregateIQ, from what I can tell from the GitLab files.

I believe if you spoke with WPA they would claim the situation was more like WPA hired AggregateIQ as developers. They worked very closely on phone applications. The Ephemeral project has heavy ties to WPA, in that some of the web-based files that would have been served up to people dialling in claimed that it was the WPA voter database. Clearly, WPA has a strong involvement with AIQ, with AIQ being either some sort of partner or a hired developer, but there is a relationship there that I believe should be looked at.

Mr. Raj Saini: Mr. Wilson noted in his biography that he has some experience as a campaign adviser in Russia, Ukraine, and Turkey. Do you have any information about AIQ's involvement in any of those countries, and what roles they might have played?

Mr. Chris Vickery: Mr. Wilson replied on that tweet string, actually, and claimed that the Russian and Turkish involvements were 20 years ago. I personally just recently found out about the Russia and Turkey involvements in his past, so I can't confirm or deny his 20 years ago claim. I know he is currently involved in a Ukrainian party, the Osnova party, and AIQ actually developed the phone app that Osnova is using right now. I don't know of direct Russian ties to AIQ, but I know of direct Ukrainian ties.

Mr. Raj Saini: One of the things we've heard in testimony is that AIQ and SCL and Cambridge Analytica have been involved in many, many elections around the world. The question I have is this, and please correct me if I'm wrong. The software that was developed was Ripon. Is that the same software that was used throughout the world, or were there different iterations or different software that was developed for different countries or places that they wanted to work in?

Mr. Chris Vickery: To be clear, Ripon is only one of the projects. However, Ripon was an early project, and I believe that many of the projects that are present on the hard drive I gave you, for example, have grown out of Ripon and sort of evolved into little ecosystems of their own. One of the themes—

Mr. Raj Saini: There may have been different iterations of that software, with a little bit of tweaking depending on where they're working and what information they had to gather, but that software is the pre-eminent software that AIQ developed for Cambridge Analytica. Is that a fair statement?

Mr. Chris Vickery: I believe that is a fair statement. I believe one of the running themes we keep running into is that much of the software is reskinned, but the engine is still significantly the same. It is something in new clothing.

Mr. Raj Saini: Okay.

In your analysis of the hard drive, have you found any evidence or indication of exactly where or what jurisdictions this software or this company was involved in anywhere?

Mr. Chris Vickery: There are definitely indicators about the U.S., Canada, the U.K., Trinidad and Tobago. There's mention of Australia. I don't know how deeply, or if there was much going on in Australia, but it's definitely mentioned.

Mr. Raj Saini: Okay.

Mr. Chris Vickery: I can't come up with any just off the top of my head in addition to those without looking more specifically for that.

Normally when I'm looking at data breaches, I try to focus on things that will resonate with North Americans because it's hard to get North Americans to care too much about very distant locales.

● (0915)

Mr. Raj Saini: Also, you recently discovered a number of apps that AIQ was running on Facebook even though they had supposedly been banned from the platform.

Do you know what these apps were? Were you given a reason that Facebook hadn't taken them down? Do you think there are still AIQ apps running on Facebook?

Mr. Chris Vickery: I believe there are probably still AIQ-influenced if not AIQ-developed apps present on Facebook under different names. I believe that's likely.

Mr. Raj Saini: You also discovered some information linking AIQ to Alex Jones and *Infowars*. Can you tell us what you found and what this connection means?

Mr. Chris Vickery: To be very clear, the only connection really was one image file that was right next to another image for an organization called For America. I know that AIQ developed a platform for For America that involved the ability to see various things the Facebook followers were saying and to recruit them. If they did the same thing for For America as they did for Breitbart, which they did do, then it stands to reason they might have done the same thing for Infowars, the website. I don't know. Other than that one image file, which I can't explain as to why it's there, I really don't know the exact relationship.

Mr. Raj Saini: Thank you very much.

The Chair: Next up for five minutes is Mr. Aboultaif.

Mr. Ziad Aboultaif (Edmonton Manning, CPC): Thank you.

I will stay on this topic a little bit, Chris. Good morning, first.

There is customization in building software for a specific reason in those specific cases that we're discussing right now. If someone builds a code for specific software to be used as a political campaign management tool, and for that they have to use certain data provided to the software builder in order to give them the tools needed for the aim of that software, will whoever is building that software be able to build it without having the data provenance available? In other words, where are the security measures here, and will these people be able to build that software without any provenance of the data?

Mr. Chris Vickery: Theoretically in the most fantastical of worlds you could build software to handle a dataset you don't have. That's just hypothetical, though. That's not reality. That's not what happens in software development. If you want to develop something quickly, profitably, on time, and to please your clients, chances are you're going to have access to a fair deal of the actual raw data.

The claims that AggregateIQ didn't have access to raw datasets, I believe, are disproven simply by what's present in the GitLab files, because there are user names, passwords, network locations to what are labelled actual databases, not fake databases.

I believe it's highly unlikely that AggregateIQ didn't have access to very large raw datasets.

Mr. Ziad Aboultaif: So chances are actually very high that availability of data and a breach of private information can never be avoided when getting into this business.

● (0920)

Mr. Chris Vickery: It can be avoided. You just have to be extremely careful and use some pre-planning to develop software carefully or have agreements in place that are strictly followed and that are audited after the fact to make sure there wasn't any unauthorized third party access.

Mr. Ziad Aboultaif: Thank you.

[*Translation*]

Mr. Jacques Gourde: It's like the chicken and egg paradox. This software was put in place because there was a potential market. Surely there is someone who has seen a potential market or orders have been given in a specific way to achieve a certain goal.

In your opinion, was it someone who saw a potential market who designed the software in question or was it the other way around, that the software was designed to order?

[*English*]

Mr. Chris Vickery: In this situation, it's my belief and understanding that there was a desired outcome and that this software was developed in response to a desired outcome. Some very powerful people wanted to influence others, win elections, and bring people's opinions and behaviours into a certain pattern. Tools were needed to accomplish that, so these tools were created for that purpose. That's my understanding, and what I believe is the most likely scenario.

[*Translation*]

Mr. Jacques Gourde: In your opinion, how many more people, percentage-wise, were reached, influenced, changed their minds or encouraged to vote than in a normal election?

[*English*]

Mr. Chris Vickery: The percentage of people in which nation?

[*Translation*]

Mr. Jacques Gourde: Other witnesses seemed to say that, regardless of the country, this system could influence an additional mass of people to vote for a different option. In percentage terms, is that a significant increase? Can it play between 2% and 7%, or is it a little less or a little more, in your opinion?

[*English*]

Mr. Chris Vickery: I believe the influence operation would not necessarily target an entire populace, but a very large percentage of people would be affected by it. That's why companies like SCL have contracts with psychological operations groups in the U.K. They affect a very large percentage of the populace and are able to change the opinions of, yes, definitely the 2% to 7%. They definitely attempted to change them, if they aren't actually changed. There is an effect on at least that small amount, yes.

[*Translation*]

Mr. Jacques Gourde: Was it profiling that targeted a portion of the population that was deemed very susceptible to the various options, that is, quite simply people who, in normal times, know more or less who to vote for, but who will make a decision at the very end of the election campaign, to the point where, if the parties repeatedly place advertising during the last 10 days of a campaign, these people can really change the game?

[*English*]

Mr. Chris Vickery: From seeing more than just this data breach and seeing other ones related to elections, I can tell you that figuring out the targets takes place well in advance of the 10 days before an election. Within the final 10 days, apps were developed specifically by AIQ to get people to make a plan to vote and follow through with that on voting day.

I'm sorry; what is the exact question there?

The Chair: Sorry, we're well past time.

I'll have to move on.

Next up for five minutes is Mr. Baylis.

● (0925)

Mr. Frank Baylis (Pierrefonds—Dollard, Lib.): Thank you, Mr. Chair.

Mr. Vickery, first of all, I'd like to thank you for this heavy lifting that you're doing and for coming back to help us understand all this. It's greatly appreciated.

You had prepared a set of notes regarding AIQ's testimony and where they were both lying and misleading. I, first of all, would ask that you submit those notes formally to our clerk, if you could.

Mr. Chris Vickery: I definitely can. I believe I did submit it to you specifically, but, yes, I can submit it to the clerk.

Mr. Frank Baylis: I want to delve into some of those lies and some of those misstatements.

First of all, Mr. Massingham stated that they had not broken any laws where they operate. That was a clear statement. You have given me examples of three places where they have broken laws. First of all, there is the way they were running U.K. data collection laws. You mentioned that they had actually written notes to themselves in their code that this was breaking the law and that they had to clear this up.

Could you expand on that?

Mr. Chris Vickery: The line in the code says where they may have broken U.K. privacy law. They don't specifically say that they did break it, but that this code, in case they did, fixes it. It's in a file called "salt the earth".

Mr. Frank Baylis: They're aware that if they're not breaking the law, they're going close to the law and that they're going to have remove this. That's right.

Mr. Chris Vickery: That's my understanding, yes. That's how I would interpret that line, yes.

Mr. Frank Baylis: With respect to caller ID spoofing, which they were doing for Americans, that is against American law. I know that you're not a lawyer, but they were aware of that and they were doing it. Is that correct?

Mr. Chris Vickery: That is my understanding, and there's even further commentary where they state that "there's no reason" that somebody halfway across the world couldn't call and influence voters. There is actually a reason why. It's illegal to have a call centre halfway across the world calling American voters to influence their opinions.

Mr. Frank Baylis: You mentioned one other area that is a great concern. They made the argument that they just had the Republican database given to them. However, when you examined this database, it was far more comprehensive, and it included a number of people such as police officers, judges, and federal agents—things that are not in the Republican data trust. Is that correct?

Mr. Chris Vickery: Let me clarify that. Those are in the Republican data trust. However, those are outside the bounds of what a normal campaign would receive. I know that because a couple of years ago I found a copy of the Republican data trust database. I have seen the contents and verified that, yes, judges, federal agents, and police officers are in there. The regular political campaign running in one of the states would not have access to those people's information.

Mr. Frank Baylis: I had asked Mr. Silvester a number of questions where he misled us with respect to a lack of coordination, or a coordination, between all these different Leave campaigners in the U.K. When I asked how they all knew about his group, he said that there was no collusion, there was no nothing. He was very clear on that. However, when I asked how would they know in the U.K., halfway around the world, about a small operation in B.C., he mentioned the website.

You did some work during the Brexit vote. You mentioned that their website—I want to just confirm this—said, "AggregateIQ: Changing the way you work with your data". Is that correct?

Mr. Chris Vickery: I believe they had nine words on their website, and those were them. They had that nine-word phrase plus a contact email address. I think it's highly unlikely that the Leave campaigners found them and decided to use their services based upon nine words on an otherwise blank website.

Mr. Frank Baylis: That's what they would lead us to believe: that they looked up and found this website, read these nine words, and emailed them, and it was all independently set up.

Mr. Chris Vickery: It seems unlikely to me.

Mr. Frank Baylis: It seems more than unlikely to me.

I have another point. Mr. Silvester mentioned that they are not data harvesters, but you did some looking at the coding. If I understand it, some of the coding undertaken by AIQ is specifically for data harvesting. Is that correct?

Mr. Chris Vickery: Yes, it is a complete fabrication to say that they are not data harvesters. They are very much data harvesters. I guess if you want to play with semantics, you could say that they were hired at points to do data harvesting, but don't consider themselves data harvesters. That doesn't mean that they're not data harvesters. They certainly have harvested data. It's a lie to say that they have not harvested data.

Mr. Frank Baylis: It's a straight-out lie, and they're playing with semantics when they say.... Whatever way they want to play it, they are doing it. They've done it. They do it. They've clearly said that they don't do it.

● (0930)

Mr. Chris Vickery: Yes.

Mr. Frank Baylis: If they say, "We ourselves aren't data harvesters, but someone hires us to do the data harvesting," that is just playing games. That is just what we call lying.

Mr. Chris Vickery: Yes.

Word games, weasel words, whatever—it's a lie.

Mr. Frank Baylis: Thank you.

The Chair: Next up is Monsieur Gourde.

[*Translation*]

Mr. Jacques Gourde: I will come back to the issue that Mr. Boulerice raised when he talked about the tip of the iceberg.

We know that there has been profiling and that software has been developed to try to categorize the population. To your knowledge, are there things that the committee didn't mention, but that should be brought to its attention? Should it be made aware of what some people intend to do in the future? Is there software being developed that we don't know why it's being developed, but could be used in an election?

[*English*]

Mr. Chris Vickery: There is election software in there. I don't know if it was ever used anywhere.

If you look in the hard drive, there's one area called vb9k and vb9k admin, something like that. It contains the skeleton if not the working prototype of a voting system, so much so that there are scripts to email people that say, "Our records indicate that you can vote by email, and here's how you would do it." I don't know if these were ever used anywhere.

There are references to the Canadian government in there. That's part of why I asked earlier whether you've ever considered using phone, email, or whatever, for voting. It appears that there was some sort of proposal made at some point, using this direct vote system.

[*Translation*]

Mr. Jacques Gourde: The further we go, the more we discover. Do you think that our electoral legislation will have to be adapted to today's new reality? What changes should we make to our legislation to protect personal information and our democracy? Should the use of these new tools be outright prohibited since, given the international context, it would be too easy to circumvent the guidelines that we could set to protect our democracy from using these tools?

[*English*]

Mr. Chris Vickery: Let's just ban the software—it's too easy to go around bans and too arbitrary to try to ban software.

I believe the answer, ultimately, will be transparency. To not allow people to hide in the shadows when they're attempting to influence populaces in ways that may or may not be unsavoury. Making it very easy to figure out who's behind a particular ad or campaign is vitally important, and the traceability of the money that paid for that campaign or ad is extremely important.

Other than that, I don't know the specifics of Canadian law on elections very well, to be honest, so I don't know what other improvements could be made.

[*Translation*]

Mr. Jacques Gourde: Do the people who use this software and all the information on the Internet really have a significant advantage over those who use only conventional tools and information provided by government agencies, in this case Elections Canada?

[*English*]

Mr. Chris Vickery: I have always believed that taking advantage of technology will give you an edge just about everywhere. It would be a philosophical belief of mine that people do have an advantage when they use the latest and greatest in software development and technology. That's just a concept I would agree with.

There are layers of taking advantage. You can use a hammer to build a house, or you can use a hammer to assault somebody. That doesn't mean you should get rid of hammers altogether.

[*Translation*]

Mr. Jacques Gourde: However, those who use this software have access to more advanced information, and even to information concerning people's private lives. If some people have access to such information, but others, who do not have the financial means to use this type of technology, use only the information provided by Elections Canada, this creates a certain injustice. You have to pay to get that information. Not all parties or all candidates can afford it. There are election spending limits, but in many cases they are never reached, simply because people can't afford them. So an injustice is being created. They are not on an equal footing in an election or in our democracy. The more this software is somewhat allowed to make progress, the more there will be a two-tier democracy.

● (0935)

[*English*]

Mr. Chris Vickery: I would say that it's a concept that can be applied to a lot of different things, and yes, it is true that the people who have more money do tend to have an advantage in elections. It's a problem that America wrestles with a lot. The Supreme Court in America has decided that money is equal to free speech, which is sacrosanct to our basic underpinnings.

It is something that is being struggled with. I don't think there's an easy answer as to how to regulate how much money and how much advantage the people with money have over the people who do not have money in an election. I don't know an easy answer to that.

[*Translation*]

Mr. Jacques Gourde: Thank you.

[*English*]

The Chair: Thank you, Mr. Gourde.

Next up is Ms. Vandenbeld.

Ms. Anita Vandenbeld (Ottawa West—Nepean, Lib.): Thank you very much for being here again. I think your testimony the last time informed much of our study and we have a much better sense of the enormity of what we're dealing with here.

After we heard from you, we did have Mr. Silvester here. I asked him about what you said about the code base having certain fingerprints. I think you mentioned that it was listed as a client. There were ID numbers that showed that SCL and AIQ were using the same code base.

What Mr. Silvester answered was, "I don't know what the researcher"—referring to you—"was referring to there, but I can say that the only information we received from SCL in the provisioning of services for SCL was specifically for those campaigns that we were assisting with." He went on to say "we don't retain any personal information from one campaign" to the other. Then he said, "we don't transfer that information to anyone, other than back to the people who provided it".

With regard to the Ripon psychosocial scoring, he said they had a "turnout score" but they didn't transfer it to anyone and also, it couldn't have gotten to anyone else through them. Also, he said that they don't keep any of the data. I'm quoting here: "We're not a data company, so we have no interest in...that."

What do you think of the credibility of his answers?

Mr. Chris Vickery: It strains the imagination to believe that somebody could state those things. They have a great deal of interest in data. There's data within that hard drive I provided you guys that proves many of his statements there incorrect. I really am surprised that he would state those things. He must have thought that I wasn't going to give the Canadian committee copies of what was present there, or he must have been at least hoping that I wouldn't, because it's simply incorrect.

Ms. Anita Vandenbeld: Thank you for having done that.

If you could send to the committee specifically—because we will be bringing them back—the things that would refute what he said, that would be very useful.

Thank you.

Mr. Chris Vickery: Mr. Baylis has copy of that, but I will send it to the whole committee.

Ms. Anita Vandenbeld: Thank you.

I will share my time with Mr. Picard.

Mr. Michel Picard (Montarville, Lib.): Thank you.

Hi again, Mr. Vickery. How are you?

Mr. Chris Vickery: I'm doing well.

Mr. Michel Picard: I have two short questions, but they're bit complicated.

I'll start with a comparison. When we look at money laundering schemes, we see that in some cases you have a bunch of companies whose structure doesn't explain the commercial activities. It's not illegal to incorporate companies, but to find 10, 15, or 20 companies in a structure that does not need that many companies is an indicator of something. It's not proof. It's an indicator.

If we look at what we have in the data you looked at, it's not illegal to have code. It's normal for a marketing company to develop code to better know their client base. What are the indicators that suggest, yes, it makes sense in certain cases, but in our case it doesn't make sense because these are the indicators that suggest, let's say, that something is fishy?

I'm asking the question because the former head of the FBI, Mr. Comey, said this week that Canada is likely to be the next target of Russian hackers. It's not an operation that you start the day after you wake up and say that it's a good idea. You have to put in place a number of things, a number of indicators that we have to look at. What would be those indicators?

● (0940)

Mr. Chris Vickery: I want to be clear that I am not an expert on international espionage by any stretch of the imagination. For the indicators that would show activity like what Mr. Comey has described, you probably are better off speaking to an expert in that field.

I can speak very clearly to and in depth upon the data that is present in the AIQ GitLab, definitely, but I wouldn't want to appear as a charlatan and make guesses at international espionage flags or indicators. I don't think I'm qualified right now to answer that.

Mr. Michel Picard: Let me relieve the pressure on your shoulders a little bit. The idea is not to see whether they are spying on us or not. If I go back to my money laundering example, from a corporate standpoint, from a financial standpoint, everyone who knows their field of work, financial experts, will say that incorporation is good and that they have to incorporate for certain activities. In this case, I find it awkward that this person, or group of persons, incorporated 15 companies. For this company, it's complicated for nothing.

When you look at what you find in your data, chances are that marketing companies do use these codes for their purposes. What suggests that it's fine in one field of work but not in another? One of the biases we have when we try to investigate something is that we put intent when there is none, but we don't see the intention when there should be one.

By practical analysis of the data, we can say that those data make sense, but in this case we don't understand why those persons use these types of data, because the context doesn't follow the purpose of the company.

Mr. Chris Vickery: Okay. I think I understand what you're getting at.

One of the original things that caught my eye when I visited the aggregateiq.com website for the first time—I didn't know who they were—was that they seemed to be in the same business, industry, or field as Cambridge Analytica. I had seen code on GitHub—different from GitLab—referencing aggregateiq.com, which had Cambridge Analytica written as a client of SCL. It all tended to be like, why are there companies in the same field all co-operating together? Don't they step on each others toes? It didn't make a lot of sense to me. That's one of the things that originally got my antenna perked up.

Another relevant item from the GitHub or GitLab files is that a U. S. politician, whose last name is "McSally", appears to have been an AIQ client—or AIQ did work on her campaign—while at the same time, I believe, being a client of Deep Root Analytics, which is another data analysis company I have found a data breach for. If there is a connection there, is it likely that the two companies were coordinating in some way to help her campaign? It seems weird to me that a campaign would use two similar companies and not have the companies talking to each other to work towards a common goal, so it further elaborates on the idea of a larger machine at work here.

Mr. Michel Picard: Thank you.

The Chair: Last up is Mr. Boulerice for three minutes.

[*Translation*]

Mr. Alexandre Boulerice: Thank you again, Mr. Vickery.

You've had some interesting interactions with the Facebook people over the past few weeks through Twitter. You raised the fact that, despite Facebook's reassuring statements, 14 AIQ applications were still active, even though they had been officially suspended by Facebook. The Facebook people answered you on Twitter, thanking you and saying they had finally suspended all 14 applications. They even dared to tell you not to hesitate to use their bounty program to report data misuse, which I find quite ironic. I don't know if you used that bounty program.

Are you less concerned now about the inappropriate way some applications use Facebook?

● (0945)

[*English*]

Mr. Chris Vickery: I am glad Facebook seems to be [*Technical difficulty—Editor*] in a good direction. I am not at all confident the infection has been totally removed. There are likely to be more apps found that are simply doing a sort of reputation laundering in that it's the same bad app under a different name and a different skin. I think that is very likely, and it will take some efforts on Facebook's part to completely rout all of the bad actors that seek to abuse the platform.

[*Translation*]

Mr. Alexandre Boulerice: As public figures, we all engage in political communication to varying degrees. We use social media for this. Most of us have accounts with many of these media. Besides, some of us are related. For my part, I have teenagers at home who are also on certain platforms.

In terms of protecting the privacy of individuals and personal information, I would like to know which of these tools, whether Facebook, Twitter, Snapchat, Instagram or others, you think is the most secure or the least likely to be used to collect data that will be used for political purposes in the future.

[*English*]

Mr. Chris Vickery: Any company that is driven by profit, which is not inherently a bad thing, is going to have an incentive to maximize that profit for their shareholders. Some would even say they have a duty to do so. Advertising and doing deep profiling and selling data are ways to maximize those profits. I don't think any of those that you mentioned are necessarily better than the other, or more privacy-centric.

I think we need to alter the industry's behaviour, and kind of change the priorities or incentives they prioritize in their heads, from just "profit, profit, profit" to "If I am less strict on privacy, I might end up getting fined by the regulators, and my profits will not be so high. I'd better protect people's information."

There's just a different carrot-and-stick dynamic that is way out of whack right now.

The Chair: That's time.

Mr. Nathaniel Erskine-Smith: Mr. Chair, we had originally planned to go in camera to discuss committee business. My one worry is that Peter and Charlie are not here. We're to do committee work in terms of recommendations, and I don't feel that comfortable, given that we've been working in a pretty non-partisan way, not having them here to do that work.

We do have some time at the moment. Perhaps Mr. Vickery has some additional time. He has indicated that he's gone in camera with the U.K. committee, and that's been helpful, to some extent. I wonder if we might take at least a half-hour and see where it goes. If Mr. Vickery is able to go in camera, we could spend some time doing that. We could also have a further discussion afterwards, if we can do any committee work otherwise.

The Chair: Yes. I was just going to bring it up about going in camera with Mr. Vickery for a certain period of time. We'll go where that takes us, I guess, and use up the time the committee wants to use up there.

Mr. Nathaniel Erskine-Smith: Great.

The Chair: As for the recommendations, the recommendations have been given by all parties. We all have them. We don't necessarily need to have them here in person to go over those, but if there are any disagreements about those recommendations—

● (0950)

Mr. Nathaniel Erskine-Smith: Assuming there are no conflicts... yes, exactly.

The Chair: —then we'll have to deal with that, I guess.

Mr. Nathaniel Erskine-Smith: Fair enough.

The Chair: To my understanding, though, it's fairly straightforward.

Mr. Vickery, you do have time, we understand, to go in camera with us in a few minutes?

Mr. Chris Vickery: Yes.

The Chair: I have a question for you just for the sake of the public. Have you been watching what's going on with the U.K. committee, including yesterday with Mr. Collins and the witness Mr. Nix? Did you have a chance to see the testimony?

Mr. Chris Vickery: I did view Mr. Nix's testimony yesterday. I had to take a few breaks to get some work done and attend a few conferences and stuff, but I did substantially view his testimony.

As to the first person you mentioned, I believe I read some of the coverage, but I don't have any special insight.

The Chair: Mr. Nix is the former head of Cambridge Analytica. To me, it was just very interesting. It kind of struck me last night, when I was watching it.... When we sit in the House until 12 o'clock at night, one thing we do is watch what the U.K. is doing; I'll admit it. The concern for me as chair—I think it's what we share as chairs on the U.S. side and in the U.K.—is that we're only looking at a couple of companies. This is my concern, I guess. Are we just scratching the surface here?

Mr. Chris Vickery: Yes. We, you, each of the committees, are scratching the surface. It is my firm belief that much more will be uncovered.

The Chair: Okay. Thank you, Mr. Vickery.

We'll suspend and then reconvene in camera in five minutes.

Mr. Chris Vickery: Sounds good.

The Chair: Thank you.

[*Proceedings continue in camera*]

Published under the authority of the Speaker of the House of Commons

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its Committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its Committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its Committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the *Copyright Act*. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a Committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the *Copyright Act*.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its Committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the House of Commons website at the following address: http://www.ourcommons.ca

Publié en conformité de l'autorité du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la *Loi sur le droit d'auteur*. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la *Loi sur le droit d'auteur*.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web de la Chambre des communes à l'adresse suivante : http://www.noscommunes.ca